AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for sharing an active secure communication session ~~with a client between a plurality of servers~~, the method comprising:

receiving a first message from ~~the~~ a client at a first server, ~~in the plurality of servers,~~ wherein the first message ~~including~~ includes a session identifier that ~~identifies~~ is associated with an active secure communication session; ~~with the client; and~~

retrieving state information using the session identifier, wherein the state information is retrieved by the first server from a database, wherein the state information includes a running message digest, wherein a second server updated the running message digest at the database as messages passed through the active secure communication session, and wherein the database, the client, the first server, and the second server are different from one another; and

using the state information to send a second message from the first server to the client through the active secure communication session.

~~if the session identifier does not correspond to an active secure communication session on the first server, establishing an active secure communication session with the client on the first server by,~~

~~attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server, wherein the state~~

~~information is retrieved from a third server which is different from the client, wherein the state information includes a session encryption key associated with the active secure communication session between the client and the second server, wherein the first server is different from the second server,~~

~~if the state information for the active secure communication session is retrieved, using the state information including the encryption keys to share the active secure communication session established between the client and the second server for subsequent communications between the client and the first server without having to set up a new secure communication session between the client and the first server, wherein the state information is purged from the second server after the state information is retrieved by the first server, and~~

~~if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.~~

2-8. (Canceled).

9. (Original) The method of claim 1, further comprising initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

10. (Currently amended) The method of claim 1, wherein ~~attempting to~~ retrievinge the state information includes authenticating and authorizing the first server.

11-12 (Canceled).

13. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for sharing an active secure communication session ~~with a client between a plurality of servers~~, the method comprising:

receiving a first message from ~~the~~ a client at a first server, ~~in the plurality of servers,~~ wherein the first message ~~including~~ includes a session identifier that ~~identifies~~ is associated with an active secure communication session; ~~with the client; and~~

retrieving state information using the session identifier, wherein the state information is retrieved by the first server from a database, wherein the state information includes a running message digest, wherein a second server updated the running message digest at the database as messages passed through the active secure communication session, and wherein the database, the client, the first server, and the second serve are different from one another; and

using the state information to send a second message from the first server to the client through the active secure communication session.

~~if the session identifier does not correspond to an active secure communication session on the first server, establishing an active secure communication session with the client on the first server by,~~

~~attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server, wherein the state information is retrieved from a third server which is different from the client, wherein the state information includes a session encryption key associated with the active secure communication~~

~~session between the client and the second server, wherein the first server is different from the second server,~~

~~if the state information for the active secure communication session is retrieved, using the state information including the encryption keys to share the active secure communication session established between the client and the second server for subsequent communications between the client and the first server without having to set up a new secure communication session between the client and the first server, wherein the state information is purged from the second server after the state information is retrieved by the first server, and~~

~~if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.~~

14-20. (Canceled).

21. (Original) The computer-readable storage medium of claim 13, wherein the method further comprises initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

22. (Currently amended) The computer-readable storage medium of claim 13, wherein ~~attempting to~~ retrievinge the state information includes authenticating and authorizing the first server.

23-24 (Canceled).

25. (Currently amended) An apparatus that shares an active secure communication session ~~with a client between a plurality of servers~~, comprising:

a receiving mechanism configured to receive a first message from a client at a first server, wherein the first message includes a session identifier that is associated with an active secure communication session; ~~at a first server in the plurality of servers, that receives a message from the client, the message including a session identifier that identifies a secure communication session with the client;~~

a retrieving mechanism configured to retrieve state information using the session identifier, wherein the state information is retrieved by the first server from a database, wherein the state information includes a running message digest, wherein a second server updated the running message digest at the database as messages passed through the active secure communication session, and wherein the database, the client, the first server, and the second server are different from one another; and

a sending mechanism configured to use the state information to send a second message from the first server to the client through the active secure communication session.

~~an examination mechanism that examines the session identifier; and~~

~~a session initialization mechanism, on the first server, wherein if the session identifier does not correspond to an active secure communication session on the first server, the session initialization mechanism is configured to establish an active secure communication session with the client by,~~

~~attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server, wherein the state information is retrieved from a third server which is different from the client, wherein the state information includes a session encryption key associated with the active secure communication~~

~~session between the client and the second server, wherein the first server is different from the second server,~~

~~if the state information for the active secure communication session is retrieved, using the state information including the encryption keys to share the active secure communication session established between the client and the second server for subsequent communications between the client and the first server without having to set up a new secure communication session between the client and the first server, and~~

~~if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.~~

26-32. (Canceled)

33. (Currently amended) The apparatus of claim 25, wherein the ~~session initialization~~retrieving mechanism is configured to authenticate and authorize the first server prior to ~~receiving~~ retrieving the state information.

34-35 (Canceled).